CLAIMS

1. A security hole diagnostic system comprising:

a script accumulation unit accumulating a plurality of scripts in a programming language describing procedures usually used by attackers for illegal access;

an operation unit making a request for a list of the plurality of scripts upon entry from a user;

a script control unit retrieving each script from the script accumulation unit upon the request from the operation unit, creating a list of an input/output parameter, a script execution condition and a test procedure described thereof, and presenting the list to the user, and executing a script that is selected by the user;

a plugin accumulation unit accumulating plugins with logics for attacking individual security holes; and

a plugin control unit, which is called by an execution of the script by the script control unit, for retrieving from the plugin accumulation unit a plugin that is specified by the script to be executed and executing the plugin on a test target computer.

2. The security hole diagnostic system according to claim 1, comprising:

a springboard simulation program including a packet

transmission/reception function, a process start/end function, a function to input/output data to/from a process, and a file transfer function; and

a springboard simulation program control unit executing the plugin on the test target computer via the springboard simulation program upon instruction from the plugin.

3. The security hole diagnostic system according to claim 1, wherein the script is constructed to have a function to allow it to call another script.

4. The security hole diagnostic system according to claim 1, wherein the script includes class concept, and

wherein the script is constructed to have a function to allow it to call another script by specifying a class name when calling the another script.

5. The security hole diagnostic system according to claim 1, comprising:

a knowledge sharing unit verifying whether the script execution condition is met,

wherein the knowledge sharing unit includes,

a deduction unit deriving new knowledge from information collected in an execution process of the script based on a deduction rule.

6. The security hole diagnostic system according to claim 5, wherein the knowledge sharing unit is constructed to have a function to execute a script for acquiring knowledge based on the deduction rule when shared knowledge is insufficient.

7. The security hole diagnostic system according to claim 2, wherein the script control unit, the plugin accumulation unit, the plugin control unit, the script accumulation unit, and the springboard simulation program control unit form a test execution unit, and the test execution unit and the operation unit are disposed separately on a network.

8. The security hole diagnostic system according to claim 1, wherein the plugin is described in an interpreter language.

9. The security hole diagnostic system according to claim 2, wherein the springboard simulation program control unit is constructed by using a protocol designed to pass firewalls.